

# Geometric representation in the theory of pseudo-finite fields

Özlem Beyarslan<sup>\*‡</sup>

Zoé Chatzidakis<sup>†‡</sup>

## Abstract

We study the automorphism group of the algebraic closure of a substructure  $A$  of a pseudo-finite field  $F$ , or more generally, of a bounded PAC field  $F$ . This paper answers some of the questions of [1], and in particular that any finite group which is geometrically represented in a pseudo-finite field must be abelian.

## Introduction

This paper investigates the relationship between model-theoretic definable closure and model-theoretic algebraic closure in certain fields. In other words: if  $F$  is a field, and  $A \subseteq F$  satisfies  $A = \text{dcl}(A)$ , what can one say of the group  $\text{Aut}(\text{acl}(A)/A)$  of restrictions to  $\text{acl}(A)$  of elements of  $\text{Aut}(F/A)$ ? When is it non-trivial? A natural assumption to add is to look at a slightly smaller group, and to impose on  $A$  that it contains an elementary substructure of  $F$ . Indeed, we certainly want to impose that our automorphisms fix  $\text{acl}^{eq}(\emptyset)$ .

This paper extends some of the results of [1], with completely new proofs, and answers some of the questions there. Here are the main results we obtain:

**Theorem 1.7.** *Let  $F$  be a bounded field,  $A = \text{dcl}(A)$  a subfield of  $F$  containing an elementary substructure of  $F$ , and let  $p$  be a prime dividing  $\#(\text{Aut}(\text{acl}(A)/A))$  and  $\#G(F)$ . Then  $p \neq \text{char}(F)$ , and  $\mu_{p^\infty} \subset F(\zeta_p)$ .*

**Theorem 1.8.** *Let  $F$  be a pseudo-finite field, [or more generally a bounded PAC field]. Assume that for some subfield  $A = \text{dcl}(A)$  of  $F$  containing an elementary substructure of  $F$ , the group  $G := \text{Aut}(\text{acl}(A)/A)$  is non-trivial. [Assume in addition that all primes dividing  $\#G$  divide  $\#G(F)$ ].*

*Then  $G$  is abelian, for any prime  $p$  dividing  $\#G$ , we have  $p \neq \text{char}(F)$ , and  $\mu_{p^\infty} \subset F$ .*

---

<sup>\*</sup>partially supported by Boğaziçi BAP 14B06P1-7840

<sup>†</sup>partially supported by PITN-2009-238381 and by ANR-13-BS01-0006

<sup>‡</sup>Both authors would like to thank the Mathematical Sciences Research Institute in Berkeley for its hospitality and support during the spring 2014, when part of this research was conducted. Research at MSRI was supported by NSF grant DMS-0932078 000

We give an example (2.5) which shows that the hypotheses on  $F_0$  cannot be weakened to assume that  $A$  contains a substructure  $F_0$  with  $\text{acl}^{eq}(\emptyset) \subset \text{dcl}^{eq}(F_0)$ . We also give a partial answer to a question of [1] on centralisers.

## 1 The results

**Notation 1.1.** Let  $F$  be a field. Throughout the paper,  $\text{dcl}$  and  $\text{acl}$  will denote the model-theoretic definable and algebraic closures, taken within the structure  $F$  or possibly some elementary extension of  $F$ .

$F^{alg}$  denotes an algebraic closure of  $F$  (i.e., an algebraically closed field containing  $F$  and minimal such),  $F^s$  its separable closure and  $G(F)$  its absolute Galois group, i.e.,  $\text{Gal}(F^s/F)$ .

If  $A \subset B$  are subfields of  $F$ , we denote by  $\text{Aut}(B/A)$  the set of automorphisms of  $B$  which preserve all  $\mathcal{L}(A)$ -formulas true in  $F$ , and by  $\text{Aut}_{\text{field}}(B/A)$  the set of (field) automorphisms of  $B$  which fix the elements of  $A$ .

We let  $\mu_{p^\infty}$  denote the group of all  $p^n$ -th roots of unity if  $p \neq \text{char}(F)$ , and  $\zeta_p$  a primitive  $p$ -th root of unity.

Let  $G_1, G_2$  be profinite groups,  $p$  a prime. We say that  $p$  divides  $\#G_1$  if  $G_1$  has a finite quotient with order divisible by  $p$ . We write  $(\#G_1, \#G_2) = 1$  if there is no prime number which divides both  $\#G_1$  and  $\#G_2$ .

**Definitions 1.2.** Let  $\mathcal{L}$  be a language,  $T$  a complete theory.

- (1) We say that the group  $G$  is *geometrically represented in the theory  $T$*  if there exists  $M_0 \prec M \models T$  and  $M_0 \subseteq A \subseteq B \subseteq M$ ,  $M$  such that  $\text{Aut}(B/A) \simeq G$ , where  $\text{Aut}(B/A)$  is the set of permutations of  $B$  which fix  $A$  and preserve the truth value of all  $\mathcal{L}(A)$ -formulas. We say that a *prime number  $p$  is geometrically represented in  $T$*  if  $p$  divides the order of some finite group  $G$  represented in  $T$ .
- (2) A field  $F$  is *bounded* if for every integer  $n$ ,  $F$  has only finitely many separable extensions of degree  $n$ . In this case we also say that  $G(F)$  is *bounded*.
- (3) A field  $F$  is *pseudo-algebraically closed*, henceforth abbreviated by *PAC*, if every absolutely irreducible variety defined over  $F$  has an  $F$ -rational point.
- (4) A field is *pseudo-finite* if it is PAC, perfect, and has exactly one extension of degree  $n$  for each integer  $n > 1$ .

**Remarks 1.3.** (Folklore) Let  $F$  be any field,  $A$  a subfield of  $F$ , and assume that  $A = \text{dcl}(A)$ . Then  $A^s \cap F$  is a Galois extension of  $A$ , equals  $\text{acl}(A)$ , and  $\text{Aut}(\text{acl}(A)/A) = \text{Gal}(A^s \cap F/A)$ . Hence the finite groups  $\text{Aut}(B/A)$  as above correspond to the finite quotients of  $\text{Gal}(A^s \cap F/A)$ .

Indeed, if  $\alpha \in \text{acl}(A)$ , let  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$  be the conjugates of  $\alpha$  over  $A$ . Then the symmetric functions in  $\{\alpha_1, \dots, \alpha_n\}$  are in  $\text{dcl}(A) = A$ , i.e.:  $\alpha$  satisfies a monic separable polynomial with

its coefficients in  $A$  and  $F$  contains all the roots of this polynomial. This shows the first assertion and the second assertion is immediate.

#### 1.4. Properties of pseudo-finite fields and bounded PAC fields.

We list some of the properties of these fields that we will use all the time, often without reference. The language is the ordinary language of rings  $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ , often expanded with parameters. Pseudo-finite fields are the infinite models of the theory of finite fields. They were studied by Ax in the 60's.

An algebraic extension of a PAC field is PAC (Corollary 11.2.5 of [3]). Theorem 20.3.3 of [3] (applied to  $K = A$ ,  $L = M = A^s \cap F$ ,  $E = F = F$ ) gives the following:

**Fact 1.** *Let  $F$  be a PAC field,  $A$  a subfield of  $F$  over which  $F$  is separable, and assume that  $A$  has a Galois extension  $C$  such that the restriction map  $G(F) \rightarrow \text{Gal}(C/A)$  is an isomorphism, and  $C \cap F = A$ . Let  $B = A^s \cap F$ ; then  $\text{Aut}_{\text{field}}(B/A) = \text{Aut}(B/A)$ .*

It suffices to notice that  $CF = F^s$ , and therefore also  $CB = B^s$ . So, if  $\varphi_0 \in \text{Aut}_{\text{field}}(B/A)$ , extend  $\varphi_0$  to  $\Phi_0 \in \text{Aut}_{\text{field}}(B^s/CA)$  by imposing  $\Phi_0$  to be the identity on  $C$ . Then  $\Phi_0$  induces the identity on  $\text{Gal}(C/A) \simeq G(B)$ . The result now follows immediately from 20.3.3 in [3]. It also has the following consequence:

**Fact 2.** *If  $F_0 \subset F$  are PAC fields of the same degree of imperfection,  $F$  is separable over  $F_0$ , and the restriction map  $G(F) \rightarrow G(F_0)$  is an isomorphism, then  $F_0 \prec F$ .*

The following remark is totally folklore, but for want of a good reference we will discuss it.

**Fact 3.** *Let  $F_0 \prec F$  and assume that  $G(F)$  is bounded. Then the restriction map  $G(F) \rightarrow G(F_0)$  is an isomorphism.*

From  $F_0 \prec F$ , it follows immediately that  $F$  is a regular extension of  $F_0$ , so that the restriction map  $G(F) \rightarrow G(F_0)$  is onto. Hence  $G(F_0)$  is bounded. Fix an integer  $n > 1$ , and let  $m(n)$  be the number of distinct separably algebraic extensions of  $F_0$  of degree  $n$ . Then there is an  $\mathcal{L}(F_0)$ -sentence which expresses this fact: that there are  $m(n)$  distinct separably algebraic extensions of  $F_0$  of degree  $n$ , and that each separably algebraic extension of degree  $n$  is contained in one of these. As  $F_0 \prec F$ ,  $F$  satisfies the same sentence, and this implies that  $F^s = F_0^s F$ , and that the restriction map  $G(F) \rightarrow G(F_0)$  is an isomorphism.

**Lemma 1.5.** *Let  $F$  be a bounded field, and  $A = \text{dcl}(A)$  a subfield of  $F$  containing an elementary substructure  $F_0$  of  $F$ , and let  $B = A^s \cap F$ . Then  $G(A) \simeq G(F_0) \times \text{Gal}(B/A)$ .*

*Proof.* Because  $G(F_0)$  is bounded and  $F_0 \prec F$ , we know that  $F^s = F_0^s F$  and the fields  $F_0^s$  and  $F$  are linearly disjoint over  $F_0$ . Hence  $B^s = F_0^s B$ , the fields  $B$  and  $AF_0^s$  are linearly disjoint over  $A$ , both are Galois extensions of  $A$ , and therefore  $G(A) = \text{Gal}(B^s/A) \simeq G(F_0) \times \text{Gal}(B/A)$ .

**Theorem 1.6.** (Koenigsmann, Thm 3.3 in [5]). *Let  $K$  be a field with  $G(K) \simeq G_1 \times G_2$ . If a prime  $p$  divides  $(\#G_1, \#G_2)$ , then there is a non-trivial Henselian valuation  $v$  on  $K$ ,  $\text{char}(K) \neq p$ , and  $\mu_{p^\infty} \subset K(\zeta_p)$ . Furthermore, if  $Kv$  denotes the residue field of  $v$  and  $\pi : G(K) \rightarrow G(Kv)$  the canonical epimorphism, then  $G(K)$  is torsion-free and  $(\#\pi(G_1), \#\pi(G_2)) = 1$ .*

**Theorem 1.7.** *Let  $F$  be a field with bounded Galois group. Assume that  $p$  is a prime number represented in  $\text{Th}(F)$  and that  $p$  divides  $\#G(F)$ . Then  $\text{char}(F) \neq p$ , and  $F(\zeta_p)$  contains  $\mu_{p^\infty}$ .*

*Proof.* Let  $F_0 \prec F$ , and  $A$  a subfield of  $F$  containing  $F_0$ , with  $A = \text{dcl}(A)$ . Let  $B = A^s \cap F$ , and assume that  $p$  divides  $\#\text{Gal}(B/A)$ , as well as  $\#G(F_0)$ . By Lemma 1.5, we know that  $G(A) \simeq G(F_0) \times \text{Gal}(B/A)$ . The result follows immediately from Theorem 1.6.

**Theorem 1.8.** *Let  $F$  be a pseudo-finite field, [or more generally a bounded PAC field]. Assume that for some subfield  $A = \text{dcl}(A)$  of  $F$  containing an elementary substructure of  $F$ , the group  $G := \text{Aut}(\text{acl}(A)/A)$  is non-trivial. [Assume in addition that all primes dividing  $\#G$  divide  $\#G(F)$ ].*

*Then  $G$  is abelian, and for any prime  $p$  dividing  $\#G$  we have  $p \neq \text{char}(F)$  and  $\mu_{p^\infty} \subset F$ .*

*Proof.* Let  $F_0 \prec F$ , and  $A = \text{dcl}(A)$  a subfield of  $F$  containing  $F_0$ , let  $B = A^s \cap F$ , and assume that  $p$  divides  $\#\text{Gal}(B/A)$ . By assumption,  $p$  divides  $\#G(F_0)$ , and by Lemma 1.5,  $G(A) \simeq \text{Gal}(B/A) \times G(F_0)$ , with  $p$  dividing the order of both factors. Let  $v$  be the Henselian valuation on  $A$  given by Theorem 1.6, and  $\pi : G(A) \rightarrow G(Av)$  the corresponding epimorphism of Galois groups. As  $F_0$  is relatively algebraically closed in  $A$ , the valuation  $v$  restricts to a Henselian valuation on  $F_0$ ; but because  $F_0$  is PAC, the only Henselian valuation on  $F_0$  is the trivial valuation ([3], Cor 11.5.6). Hence  $F_0 \subseteq Av$ , and by Henselianity of  $v$ ,  $F_0^s \cap Av = F_0$ . Hence the map  $\pi$  is an isomorphism between  $G(A)$  and  $G(F_0)$ . It follows that  $\text{Gal}(BF_0^s/AF_0^s)$  is contained in  $\text{Ker}(\pi)$ , the inertia subgroup of  $v$ , and its order is prime to the characteristic. Hence  $A^s$  is the composite of the purely residual extension  $AF_0^s$  of  $A$ , and the totally ramified extension  $B$  of  $A$ . The characteristic of  $F$  does not divide  $\#\text{Gal}(B/A)$ , and this implies that  $\text{Gal}(B/A)$  is abelian: indeed, by Theorem 5.3.3 and § 5.3 in [2], we have

$$\text{Gal}(B/A) \simeq \text{Gal}(BF_0^s/AF_0^s) \simeq \text{Hom}(\Gamma(A^s)/\Gamma(AF_0^s)), (Aw)^{s^\times},$$

where  $w$  denotes the unique extension of  $v$  to  $A^s$ , and  $\Gamma(A^s)$ ,  $\Gamma(AF_0^s)$  the value groups  $w(A^s)$  and  $w(AF_0^s) = v(A)$ .

We also know that  $\mu_{p^\infty} \subset F(\zeta_p)$ . Assume first that  $G(F)$  is abelian. Then so is  $G(A)$ , and therefore any field between  $A$  and  $A^s$  is a Galois extension of  $A$ . In particular, because  $p$  divides  $\#G$ , some element  $\gamma \in v(A)$  is not divisible by  $p$  in  $v(A)$ . Thus, if  $v(a) = \gamma$ , then  $a^{1/p} \in A^s$ , and generates a Galois extension of  $A$ : this implies that  $\zeta_p \in A$ , and by the above that  $\mu_{p^\infty} \subset F_0$ . Assume now that  $G(F)$  is arbitrary, and that  $\zeta_p \notin F_0$ . Then there is some  $\sigma \in G(F)$  such that  $\sigma(\zeta_p) \neq \zeta_p$ , and the subgroup generated by  $\sigma$  has order divisible by  $p$  (here we use that  $p$  divides  $\#G(F)$ ). Then the restriction of  $\sigma$  to  $A^s$  commutes with all elements of  $\text{Gal}(A^s/F_0^s A)$ , and so we may apply the previous result to the PAC field  $K$ , subfield of  $F^s$  fixed by  $\sigma$ , and its elementary substructure  $K_0$ , subfield of  $F_0^s$  fixed by  $\sigma$ , to deduce that  $\zeta_p \in K_0$ , which contradicts our choice of  $\sigma$ .

**Corollary 1.9.** *Let  $F$  be a pseudo-finite field, or a bounded PAC field with  $\#G(F)$  divisible by every prime number. Then every group represented in  $\text{Th}(F)$  is abelian. Furthermore, if  $p$  is a prime represented in  $\text{Th}(F)$ , then  $\mu_{p^\infty} \subset F$  and  $p \neq \text{char}(F)$ .*

**Corollary 1.10.** *Let  $F$  be a pseudo-finite field such that if  $p$  is a prime number  $\neq \text{char}(F)$ , then  $\mu_{p^\infty} \not\subset F$ . Then definable closure and algebraic closure agree on subsets of  $F$  containing an elementary substructure of  $F$ .*

## 2 Other comments and remarks

**2.1.** As was shown in Theorem 7 of [1], if  $F$  is a pseudofinite field not of characteristic  $p$  and containing  $\mu_{p^\infty}$ , then every abelian  $p$ -group is represented in  $\text{Th}(F)$ . Moreover, as the class of groups represented in  $\text{Th}(F)$  is stable by direct product (Remark 12 in [1]), it follows that which abelian groups are represented in  $\text{Th}(F)$  is entirely determined by  $\text{char}(F)$  and by which  $\mu_{p^\infty}$  are contained in  $F$ .

The proof given in [1] easily generalises to any perfect PAC field  $F$ , as they do have a notion of amalgamation over models, and the construction did not use the pseudo-finiteness of  $F$ , only the fact that it is PAC. We give here again the construction of a field with absolute Galois group containing a cartesian product, it will be used in the construction of example 2.5.

**2.2. The construction.** Let  $F$  be a perfect field containing all primitive roots of unity, and consider the field  $K$  of generalized power series  $F^s((t^\mathbb{Q}))$  over  $F^s$ . Its members are formal sums  $\sum_\gamma a_\gamma t^\gamma$ , with  $\gamma \in \mathbb{Q}$ ,  $a_\gamma \in F^s$ , satisfying that  $\{\gamma \mid a_\gamma \neq 0\}$  is well-ordered. Then  $K$  is algebraically closed. We define an action of  $G(F)$  on  $K$  by setting

$$\sigma\left(\sum_\gamma a_\gamma t^\gamma\right) = \sum_\gamma \sigma(a_\gamma) t^\gamma.$$

So, the subfield of  $K$  fixed by  $G(F)$  coincides with  $F((t^\mathbb{Q}))$ . For each  $n \in \mathbb{N}$  not divisible by the characteristic of  $F$ , choose a primitive  $n$ -th root of unity  $\zeta_n$ , and choose them in a compatible way, i.e., such that  $\zeta_{nm}^m = \zeta_n$ . Let  $\sigma \in \text{Aut}(K)$  be defined by defining  $\sigma(t^{1/n}) = \zeta_n t^{1/n}$  for  $n$  prime to the characteristic, and if  $q$  is a power of the characteristic, then  $\sigma(t^{1/q}) = t^{1/q}$ ; extend  $\sigma$  to the multiplicative group  $t^{1/n}$ ,  $n \in \mathbb{Z}$ , and then to  $K$  by setting

$$\sigma\left(\sum_\gamma a_\gamma t^\gamma\right) = \sum_\gamma a_\gamma \sigma(t^\gamma).$$

Let  $A$  be the subfield of  $K$  fixed by  $G(F)$  and by  $\sigma$ . Then  $G(A) \simeq G(F) \times \langle \sigma \rangle = G(F) \times \hat{\mathbb{Z}}$ .

**2.3. Remark.** Let  $F$  be a perfect PAC field, and let  $A$  be the field constructed above. So  $A$  contains a copy of  $F$  and is contained in  $F((t^\mathbb{Q}))$ ; as  $F((t^\mathbb{Q}))$  is a regular extension of  $F$ , it follows that  $F$  has an elementary extension  $F^*$  which contains  $B = A^s \cap F((t^\mathbb{Q}))$ . Then  $\text{Aut}(B/A) = \text{Gal}(B/A) \simeq \hat{\mathbb{Z}}$ . This proof already appeared in [1] (Thm 7).

**2.4. Comment 1.** The proof of Lemma 1.5 works exactly in the same fashion as soon as the field  $A$  contains enough information about  $G(F)$ , more precisely: Assume  $A$  contains  $\text{acl}(\emptyset)$ , and that for each finite extension  $L$  of  $F$ , there is  $\alpha$  such that  $L = F(\alpha)$  and the minimal polynomial of  $\alpha$  over  $F$  has its coefficients in  $A = \text{dcl}(A)$ ; then  $A$  has a Galois extension  $C$

which is linearly disjoint from  $F$  over  $A$ , and is such that  $CF = F^s$ . Then again one has  $G(A) \simeq G(F) \times \text{Gal}(A^s \cap F/A)$ . The proof of Theorems 1.7 goes through verbatim.

We were trying to weaken the hypotheses on  $A$ , and a natural weaker assumption is to assume that  $A$  contains a subfield  $F_0$  such that  $\text{acl}^{eq}(\emptyset) \subseteq \text{dcl}^{eq}(F_0)$  and  $\text{acl}(F_0) = F_0$ . However the proof of Theorem 1.8 used in an essential way the fact that  $F_0$  was PAC. The example below shows that this condition is not sufficient.

## 2.5. An example showing that the hypothesis of containing an elementary substructure is necessary.

Let  $A_0$  be a field containing  $\mathbb{Q}^{alg}$ , and consider  $A_0^{alg}((t^{\mathbb{Q}}))$ ; define actions of  $G(A_0)$  and of  $\sigma$  on  $A_0^{alg}((t^{\mathbb{Q}}))$  as above. Then  $G(A_0((t))) \simeq G(A_0) \times \langle \sigma \rangle$ . Let  $F_0 = \mathbb{Q}^{alg}((t))$ , the subfield of  $\mathbb{Q}^{alg}((t^{\mathbb{Q}}))$  fixed by  $\sigma$ , and  $A = A_0((t))$ . Then  $G(F_0) \simeq \hat{\mathbb{Z}}$ , and  $A$  contains  $F_0$ . Furthermore, because  $G(F_0)$  is isomorphic to  $\hat{\mathbb{Z}}$ , there is a pseudo-finite field  $F$  which is a regular extension of  $F_0$  (this follows easily from Thm 23.1.1 in [3]), so that the restriction map  $G(F) \rightarrow G(F_0)$  is an isomorphism. By Corollary 3.1 in [4], the theory of  $F$  eliminates imaginaries in the language augmented by constants for elements of  $F_0$ . As  $F_0$  also contains  $\text{acl}(\emptyset) = \mathbb{Q}^{alg}$ , it follows that  $\text{acl}^{eq}(\emptyset) \subset \text{dcl}^{eq}(F_0)$ . Furthermore, by standard results on pseudo-finite fields,  $F$  has an elementary extension  $F^*$  which contains  $A$  and is a regular extension of  $B = A^{alg} \cap A_0^{alg}((t))$ . Then  $\text{Gal}(B/A) = \text{Aut}(B/A) \simeq G(A_0)$ .

This shows that the hypothesis of  $A$  containing an elementary substructure of  $F^*$  cannot be weakened to  $A$  containing a substructure  $F_0$  with  $\text{acl}^{eq}(\emptyset) \subset \text{dcl}^{eq}(F_0)$  and  $F_0 = \text{acl}(F_0)$ .

**2.6. Comment 2.** One can wonder what happens for a bounded PAC field  $F$  with  $G(F)$  not divisible by all primes. If  $S$  is the set of prime numbers  $\neq \text{char}(F)$  and which do not divide  $\#G(F)$ , and if  $H$  is a projective  $S$ -group (i.e., the order of the finite quotients of  $S$  are products of members of  $S$ ), then  $G(F) \times H$  is a projective profinite group. Hence  $F$  has a regular extension  $K$  which is PAC and with  $G(K) \simeq G(F) \times H$  (Thm 23.1.1 in [3]). We may also impose, if the characteristic is positive, that  $K$  and  $F$  have the same degree of imperfection. As  $K$  is a regular extension of  $F$ , the restriction map  $G(K) \rightarrow G(F)$  restricts to an isomorphism on  $G(F) \times (1)$ , and sends  $(1) \times H$  to 1. Let  $K_1$  be the subfield of  $K^s$  fixed by  $G(F) \times (1)$ . Then  $K_1$  is PAC, and because the restriction map  $G(K_1) \rightarrow G(F)$  is an isomorphism, we have  $F \prec K_1$ . If  $A$  is the subfield of  $K^s$  fixed by  $G(F) \times H$ , then  $A \subset F_1$ , and  $\text{Gal}(F_1/A) = \text{Aut}(F_1/A) \simeq H$ .

**2.7. Comment 3.** Let  $K$  be a field,  $G = \text{Aut}(K(t)^{alg}/K(t))$ , and  $\sigma \in G$ . Consider  $G(\sigma)$  the centralizer of  $\sigma$  in  $G$ . Let  $B$  be the subfield of  $K(t)^{alg}$  fixed by  $\sigma$ ,  $F_0 = K^{alg} \cap B$ , and assume that  $F_0$  is pseudo-finite. Because  $G(B) = \langle \sigma \rangle$  projects onto  $G(F_0) \simeq \hat{\mathbb{Z}}$ , we have  $G(B) \simeq \hat{\mathbb{Z}}$ , and  $F_0$  has an elementary extension  $F$  which is a regular extension of  $B$ . We are interested in  $\text{Aut}_{\text{field}}(B/F_0(t))$ ; as  $B \cap F_0^{alg} = F_0$ ,  $B$  is linearly disjoint from  $F_0^{alg}(t)$  over  $F_0(t)$ , and therefore  $\text{Aut}_{\text{field}}(B/F_0(t)) = \text{Aut}(B/F_0(t))$ , and its elements commute with  $\sigma$ .

Let  $H$  be a closed subgroup of  $G(\sigma)$  such that  $H \cap \langle \sigma \rangle = 1$ . Then Theorem 1.8 tells us that  $H$  is abelian, and that the subfield  $A$  of  $B$  fixed by  $H$  has a non-trivial Henselian valuation  $v$ , which is trivial on  $F_0$ . Furthermore, if  $p$  divides  $\#H$ , then  $p \neq \text{char}(F_0)$ , and  $\mu_{p^\infty} \subset F_0$ . We take the unique extension of  $v$  to  $A^s$  (and also call it  $v$ ); then the residue fields  $Av$  and  $Bv$  equal  $F_0$ , and  $(Av)^s = F_0^s$ . Furthermore  $H$  is procyclic, because  $\Gamma(A) \simeq \mathbb{Z}$ , and  $H \simeq \text{Hom}(\mathbb{Q}/\mathbb{Z}, F_0^{s \times})$ .

The restriction of  $v$  to  $F_0(t)$  corresponds to a point of  $\mathbb{P}^1(F_0)$  (because  $Av = F_0$ ), i.e., either  $v(t - a) = 1$  for some  $a \in F_0$ , or  $v(t) = -1$ . On the other hand, the field  $B$  can carry at most one Henselian valuation (see Thm 4.4.1 of [2]). It follows that  $\text{Aut}_{\text{field}}(B/F_0(t))$  is abelian, procyclic. Hence  $G(\sigma)$  splits as  $\langle \sigma \rangle \times \langle \tau \rangle$ . The result generalises to any bounded PAC subfield  $F_0$  of  $K$ , with exactly the same reasoning.

This gives a partial answer to Questions 15 and 16 of [1].

Consider  $K = \mathbb{Q}$ , and endow  $G(\mathbb{Q}(t))$  with the Haar measure. Then the set  $\{\tau \in G(\mathbb{Q}) \mid \mathbb{Q}^{alg}(\tau) \text{ is pseudofinite}\}$  has measure 1, see Thm 18.6.1 in [3]. Here  $\mathbb{Q}^{alg}(\tau)$  denotes the subfield of  $(\mathbb{Q}^{alg})$  fixed by  $\sigma$ . Moreover, it is easy to see that with probability 1,  $\mathbb{Q}^{alg}(\sigma)$  does not contain  $\mu_p$  for any prime  $p$ . Hence, if  $\sigma$  is any extension of  $\tau$  to  $\mathbb{Q}(t)^{alg}$ , and  $B = \mathbb{Q}(t)^{alg}(\sigma)$ , then  $\text{Aut}(B/F_0(t)) = 1$ .

### Addresses of the authors

Boğaziçi University  
Faculty of Arts and Science  
Department of Mathematics  
34342, Bebek-Istanbul  
Turkey

CNRS (UMR 8553) - Ecole Normale Supérieure  
45 rue d'Ulm  
75230 Paris cedex 05  
France

## References

- [1] Ö. Beyarslan, E. Hrushovski, On algebraic closure in pseudo-finite fields, *Journal of Symbolic Logic* **77** (2012) 1057-1066.
- [2] A. J. Engler, A. Prestel, *Valued Fields*, Springer Monographs in Mathematics, **11**, Springer-Verlag Berlin, 2005.
- [3] M. Fried, M. Jarden, *Field Arithmetic*, Erg. Math. **11**, Springer-Verlag Berlin, 2005.
- [4] E. Hrushovski, Pseudo-finite fields and related structures, in: *Model Theory and Applications*, Bélair et al. ed., Quaderni di Matematica Vol. 11, Aracne, Rome 2005, 151 – 212.
- [5] J. Koenigsmann, Products of Absolute Galois Groups, *Int. Math. Res. Not.*(2005), no 24, 1465 – 1486.